Early Adopters

Incident Object Description and Exchange Format

The Gathering

- Gathering of Swedish University CSIRTs (+10)
- Seeking cooperation with SUNET-CERT
  - Coordination
  - Contact information, f.ex. TF-CSIRT, LEA, et.al
  - Statistical purposes
  - Goal to have an uniform view on Incident Handling capabilities
- Information about different Ticketing Systems
- IODEF adoptation

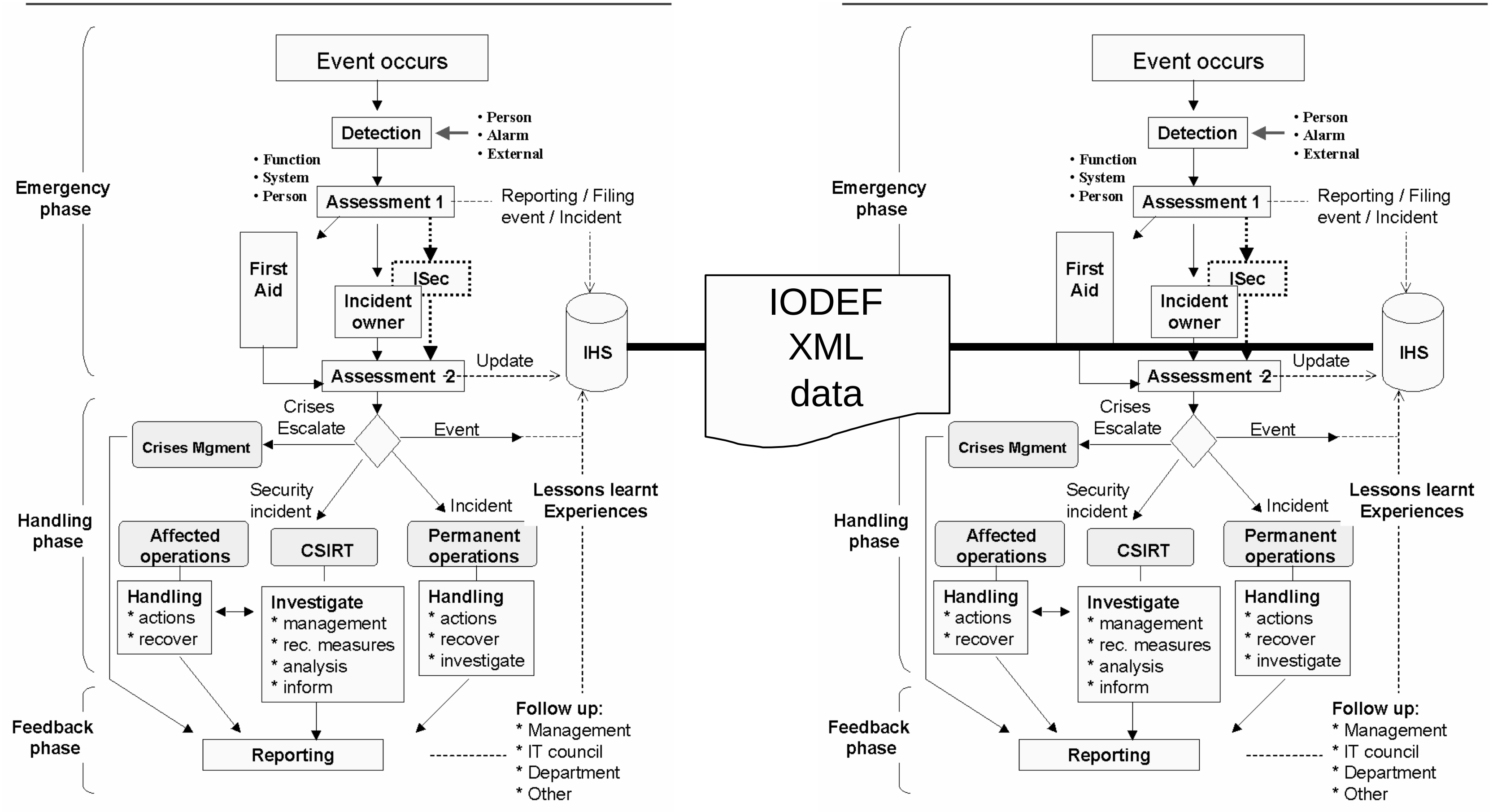
Why IODEF format exchange?

- Exchanging Incident Information between CSIRTs
- Sharing of Incident Information in order to:
  - Collaborate / Co-ordinate on Incident Handling
  - Collate incident data (check perpetrator's hits/ different victims)
  - Statistical purposes
- Exchange of single or multiples incident(s)
- Standardised format

IODEF exchange

CSIRT A

CSIRT B



Emergency phase

Event occurs

Detection

• Person
• Alarm
• External

• Function
• System
• Person

Assessment 1

Reporting / Filing event / Incident

First Aid

ISec

Incident owner

IHS

Assessment 2

Update

Handling phase

Crises Escalate

Crises Mgment

Event

Security incident

Incident

Lessons learnt Experiences

Affected operations

CSIRT

Permanent operations

Handling
* actions
* recover

Investigate
* management
* rec. measures
* analysis
* inform

Handling
* actions
* recover
* investigate

Feedback phase

Reporting

Follow up:
* Management
* IT council
* Department
* Other

IODEF XML data

Emergency phase

Event occurs

Detection

• Person
• Alarm
• External

• Function
• System
• Person

Assessment 1

Reporting / Filing event / Incident

First Aid

ISec

Incident owner

IHS

Assessment 2

Update

Handling phase

Crises Escalate

Crises Mgment

Event

Security incident

Incident

Lessons learnt Experiences

Affected operations

CSIRT

Permanent operations

Handling
* actions
* recover

Investigate
* management
* rec. measures
* analysis
* inform

Handling
* actions
* recover
* investigate

Feedback phase

Reporting

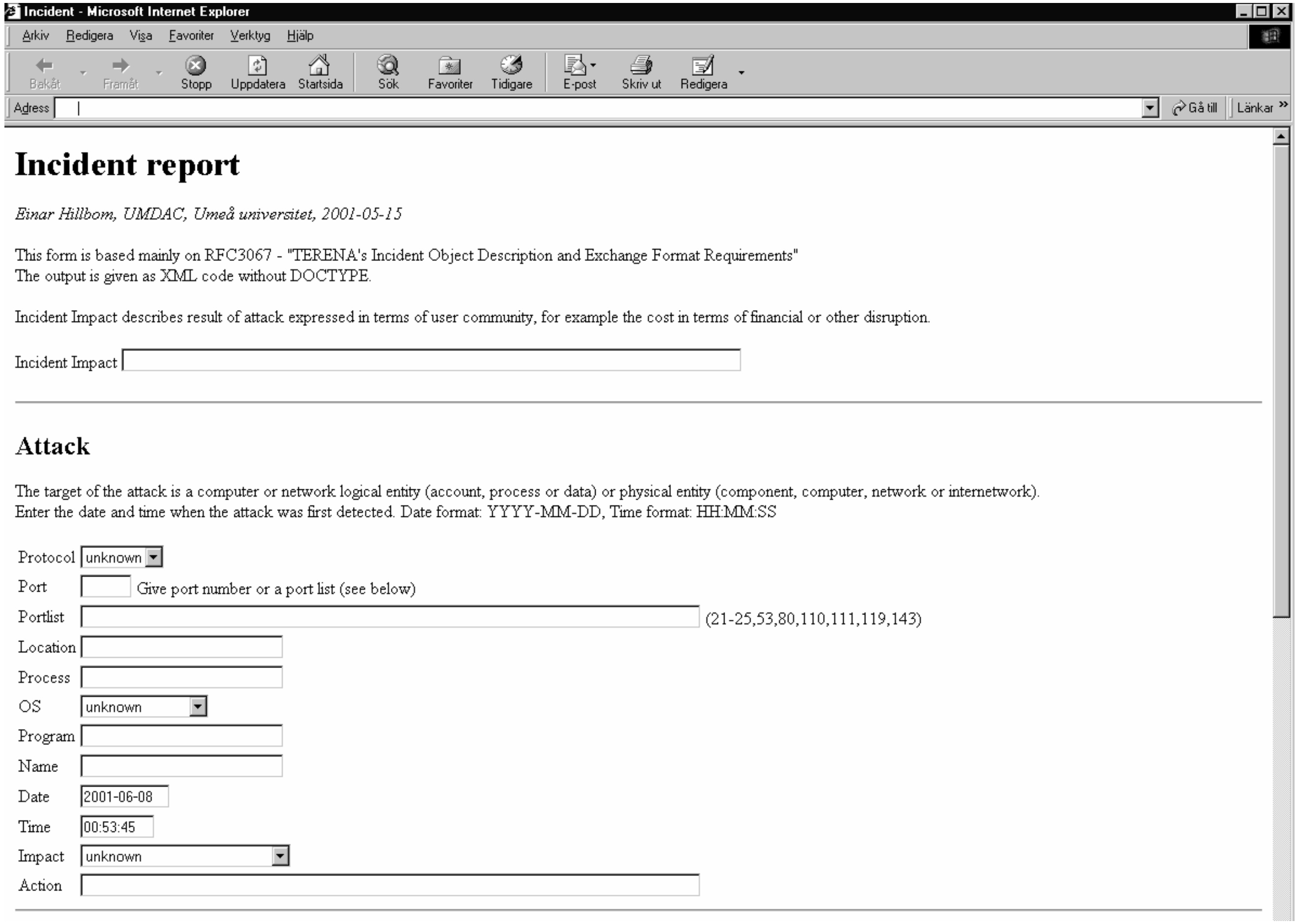
Follow up:
* Management
* IT council
* Department
* Other

IHS = Incident Handling/Tracking System

Conclusion

- Decided to try to adopt IODEF and IDMEF
- Implement IODEF features in Request-Tracker
- Web form for registering incidents (open for all)
  (actual status: test and demo purposes only. See nxt slide)
- All data entered is readable for all University CSIRTs (no secrets)

Incident Report acc. IODEF



Incident report

Einar Hillbom, UMDAC, Umeå universitet, 2001-05-15

This form is based mainly on RFC3067 - "TERENA's Incident Object Description and Exchange Format Requirements"
The output is given as XML code without DOCTYPE.

Incident Impact describes result of attack expressed in terms of user community, for example the cost in terms of financial or other disruption.

Incident Impact

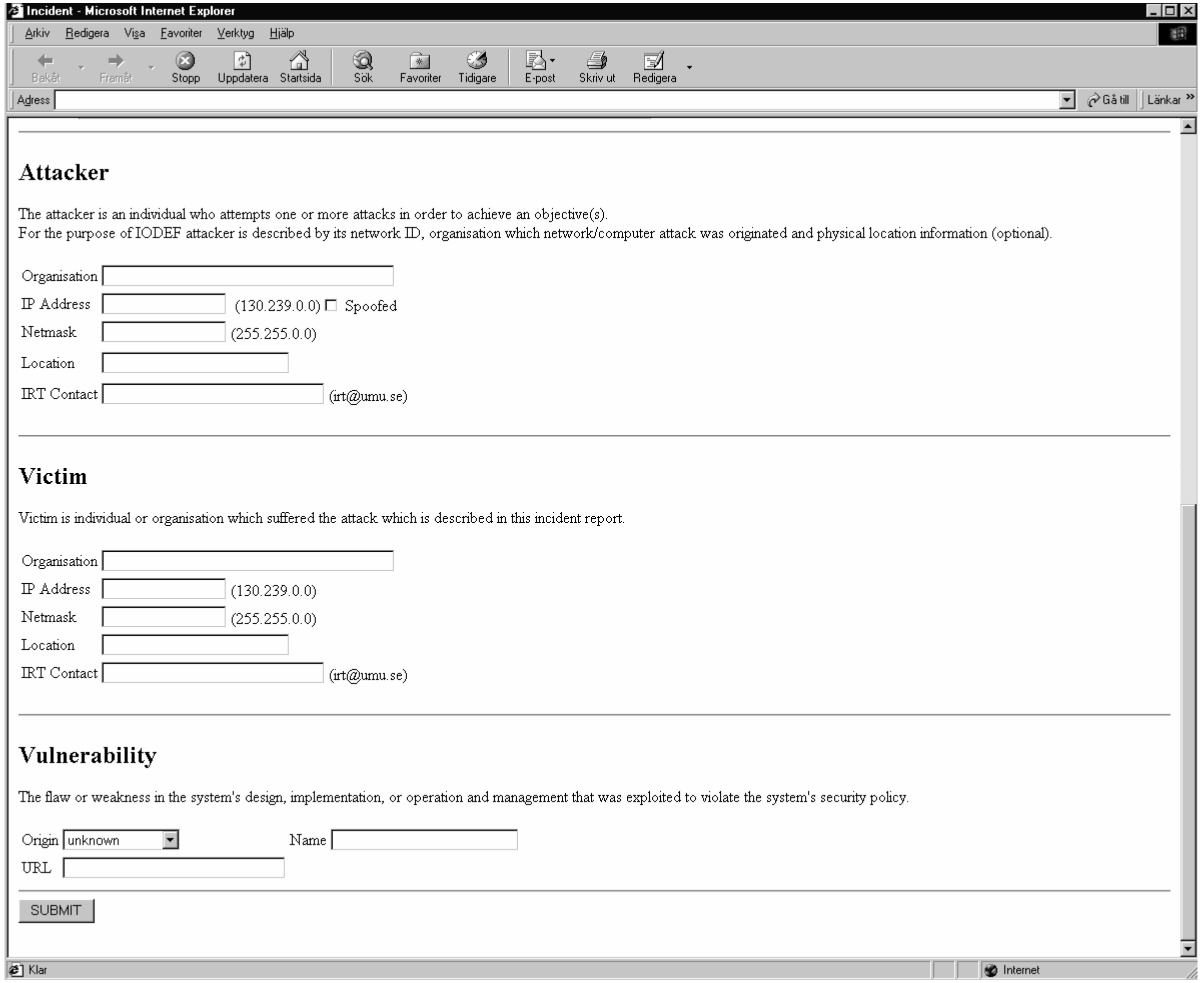
Attack

The target of the attack is a computer or network logical entity (account, process or data) or physical entity (component, computer, network or internetwork).
Enter the date and time when the attack was first detected. Date format: YYYY-MM-DD, Time format: HH:MM:SS

Protocol	unknown	
Port		Give port number or a port list (see below)
Portlist		(21-25,53,80,110,111,119,143)
Location		
Process		
OS	unknown	
Program		
Name		
Date	2001-06-08	
Time	00:53:45	
Impact	unknown	
Action		

URL: **http://irt.umdc.umu.se/cgi-bin/IRT/incident.cgi**

Incident Report acc. IODEF (cont’d)



Attacker

The attacker is an individual who attempts one or more attacks in order to achieve an objective(s).
For the purpose of IODEF attacker is described by its network ID, organisation which network/computer attack was originated and physical location information (optional).

Organisation

IP Address (130.239.0.0) □ Spoofed

Netmask (255.255.0.0)

Location

IRT Contact (irt@umu.se)

Victim

Victim is individual or organisation which suffered the attack which is described in this incident report.

Organisation

IP Address (130.239.0.0)

Netmask (255.255.0.0)

Location

IRT Contact (irt@umu.se)

Vulnerability

The flaw or weakness in the system's design, implementation, or operation and management that was exploited to violate the system's security policy.

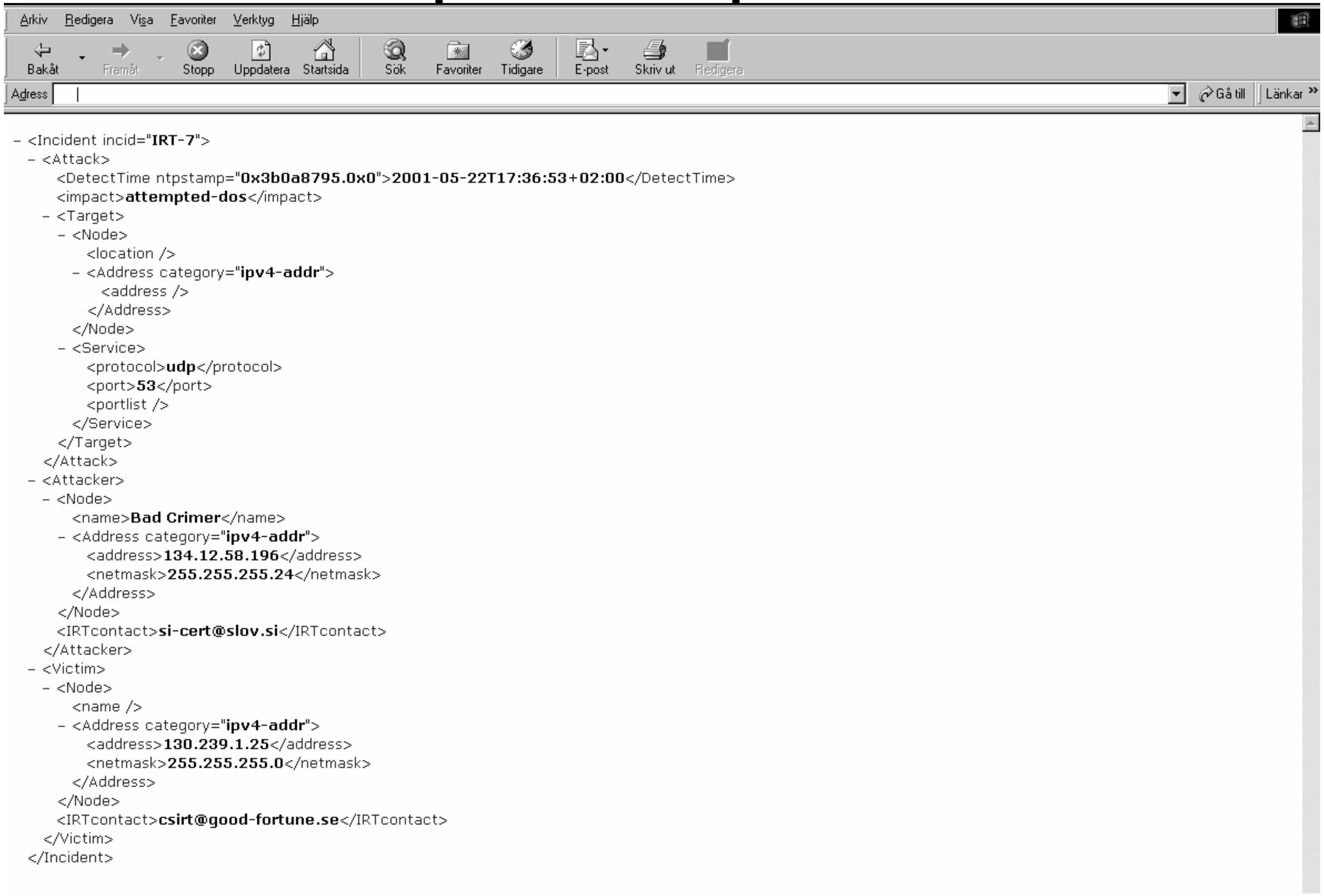
Origin unknown Name

URL

SUBMIT

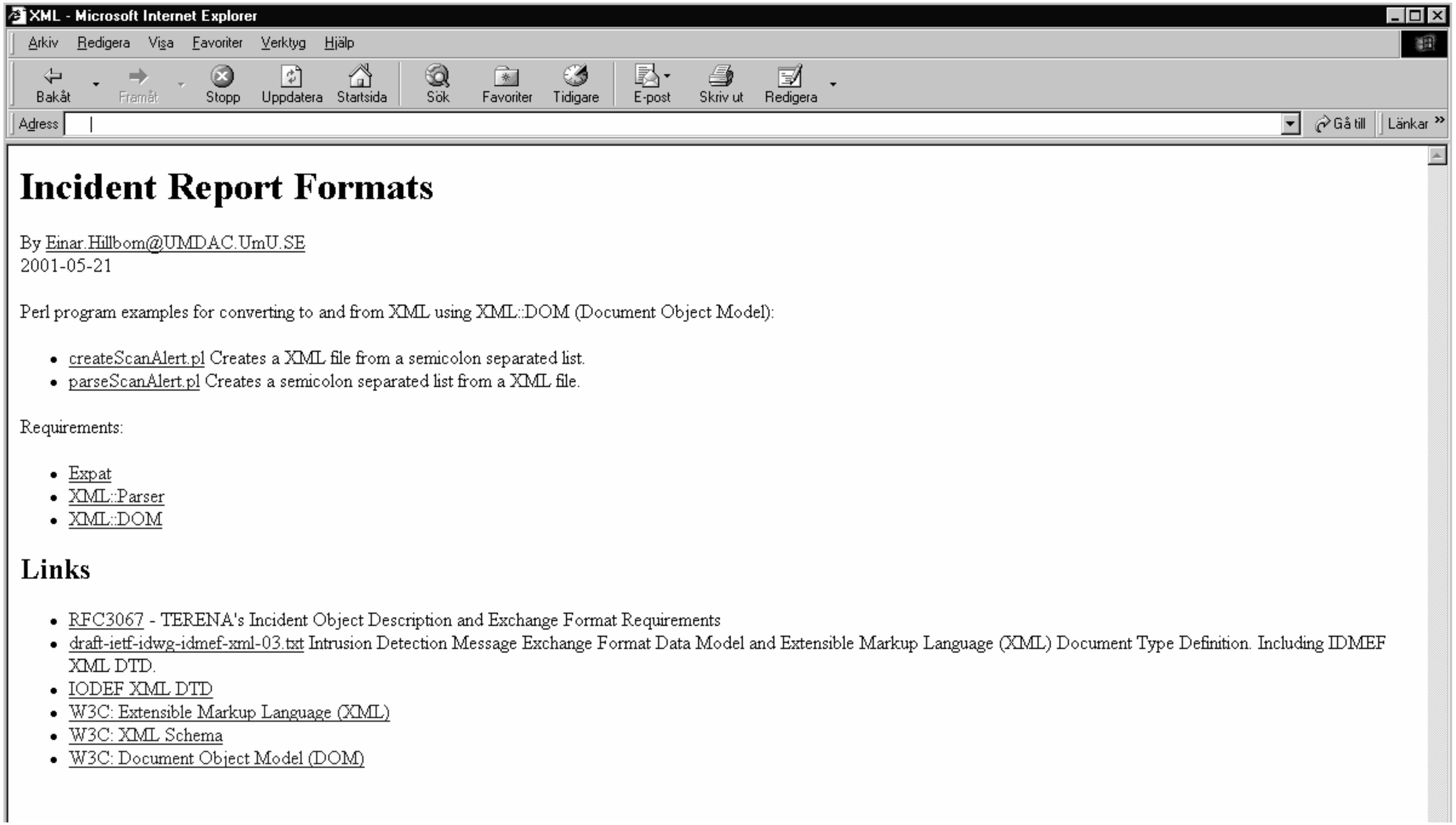
URL: http://irt.umdac.umu.se/cgi-bin/IRT/incident.cgi

Incident Report Output



```
- <Incident incid="IRT-7">
  - <Attack>
      <DetectTime ntpstamp="0x3b0a8795.0x0">2001-05-22T17:36:53+02:00</DetectTime>
      <impact>attempted-dos</impact>
    - <Target>
      - <Node>
          <location />
        - <Address category="ipv4-addr">
            <address />
          </Address>
        </Node>
      - <Service>
          <protocol>udp</protocol>
          <port>53</port>
          <portlist />
        </Service>
      </Target>
    </Attack>
  - <Attacker>
    - <Node>
        <name>Bad Crimer</name>
      - <Address category="ipv4-addr">
          <address>134.12.58.196</address>
          <netmask>255.255.255.24</netmask>
        </Address>
      </Node>
      <IRTcontact>si-cert@slov.si</IRTcontact>
    </Attacker>
  - <Victim>
    - <Node>
        <name />
      - <Address category="ipv4-addr">
          <address>130.239.1.25</address>
          <netmask>255.255.255.0</netmask>
        </Address>
      </Node>
      <IRTcontact>csirt@good-fortune.se</IRTcontact>
    </Victim>
  </Incident>
```

Einar Hillbom www-page


XML - Microsoft Internet Explorer
Arkiv Redigera Visa Favoriter Verktyg Hjälp
Bakåt Framåt Stopp Uppdatera Startsida Sök Favoriter Tidigare E-post Skriv ut Redigera
Adress
Gå till Länkar »

Incident Report Formats

By Einar.Hillbom@UMDAC.UmU.SE
2001-05-21

Perl program examples for converting to and from XML using XML::DOM (Document Object Model):

- createScanAlert.pl Creates a XML file from a semicolon separated list.
- parseScanAlert.pl Creates a semicolon separated list from a XML file.

Requirements:

- Expat
- XML::Parser
- XML::DOM

Links

- RFC3067 - TERENA's Incident Object Description and Exchange Format Requirements
- draft-ietf-idwg-idmef-xml-03.txt Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition. Including IDMEF XML DTD.
- IODEF XML DTD
- W3C: Extensible Markup Language (XML)
- W3C: XML Schema
- W3C: Document Object Model (DOM)

URL: http://personliga.umdac.umu.se/einar.hillbom/IRT/

How to report security incidents in IODEF?

- Reporting a port scan as:
  - Alert IDMEF
  - IncidentAlert IODEF
- Complete investigations
  - Incident IODEF
- Propose how to use IODEF and give practical examples

Wishlist

- Practical examples how to use IODEF
- An uniform method to classify security incidents
  - What is considered to be a port scan?
  - What if an attack consists of a scan and a DoS?